La nomenclature logicielle dans l'industrie automobile

Charlie Hart
Hitachi America Ltd - Groupe de recherche et développement

24 mars 2022

Présentation de l'orateur

HITACHI
Inspire the Next

Charlie Hart
Hitachi America Ltd.

Postes actuels

- Analyste principal, Sécurité, Hitachi America R&D
- Président, Groupe d'affinité des fournisseurs Auto-ISAC, Groupe de travail SBOM

Postes antérieurs

- Vice-président senior, Ingénierie logicielle et des solutions, Hitachi Data Systems
- Vice-président, Ingénierie OSS, Savvis
- Directeur principal, Ingénierie logicielle, Sun Microsystems
- Vice-président, Ingénierie de l'infrastructure logicielle, Veritas Software
- Vice-président, Sécurité des systèmes/Ingénierie des services, StorageNetworks
- Vice-président, Systèmes et services technologiques, Massachusetts Financial Services
- Spécialiste de projet/analyste-programmeur, Services logiciels, Digital Equipment Corporation

Éducation

- Baccalauréat ès arts, anglais - Boston College

Ordre du jour

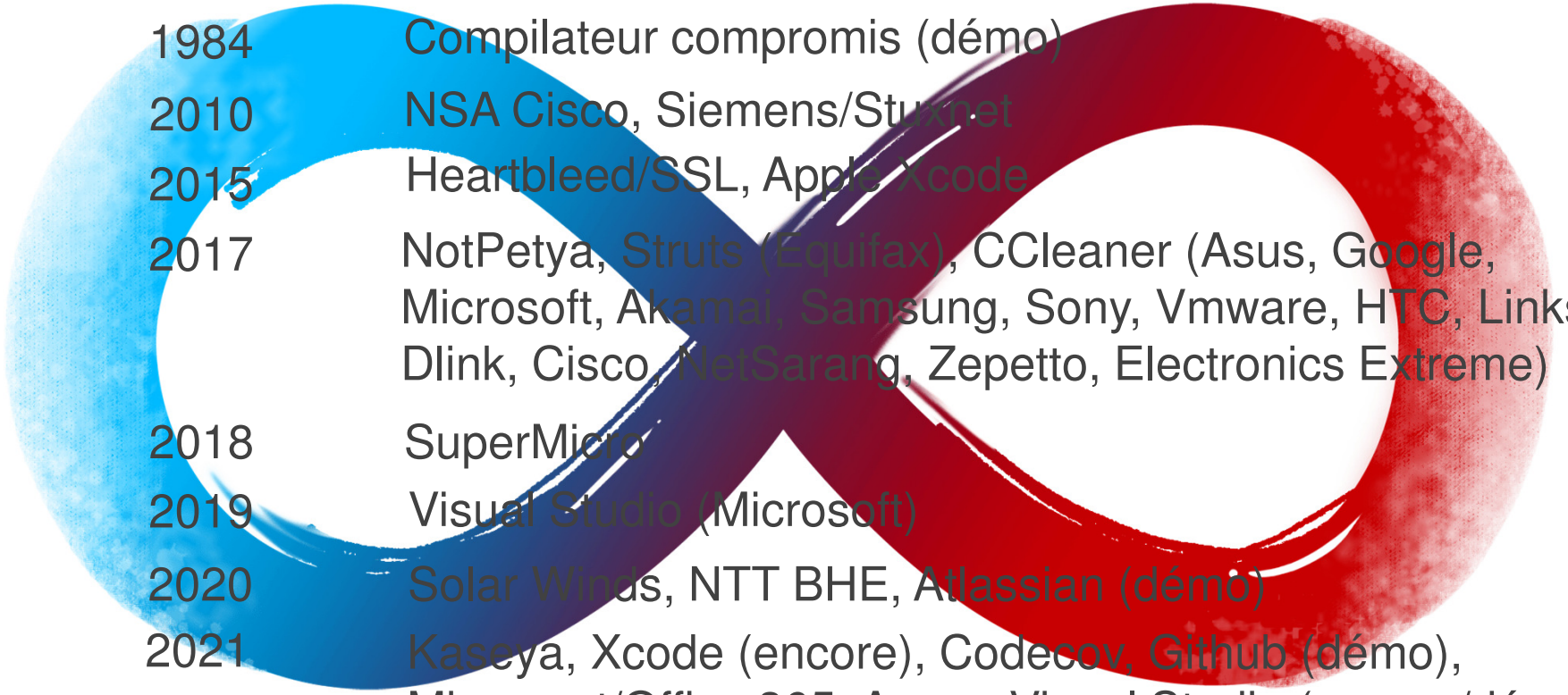
HITACHI
Inspire the Next

- Pourquoi le SBOM est important pour l'industrie automobile
- Auto-ISAC et SBOM - Historique, détails et statut
- Prochaines étapes

Pourquoi le SBOM est important pour l'industrie automobile

Attaques de la chaîne logistique logicielle - Un bref historique

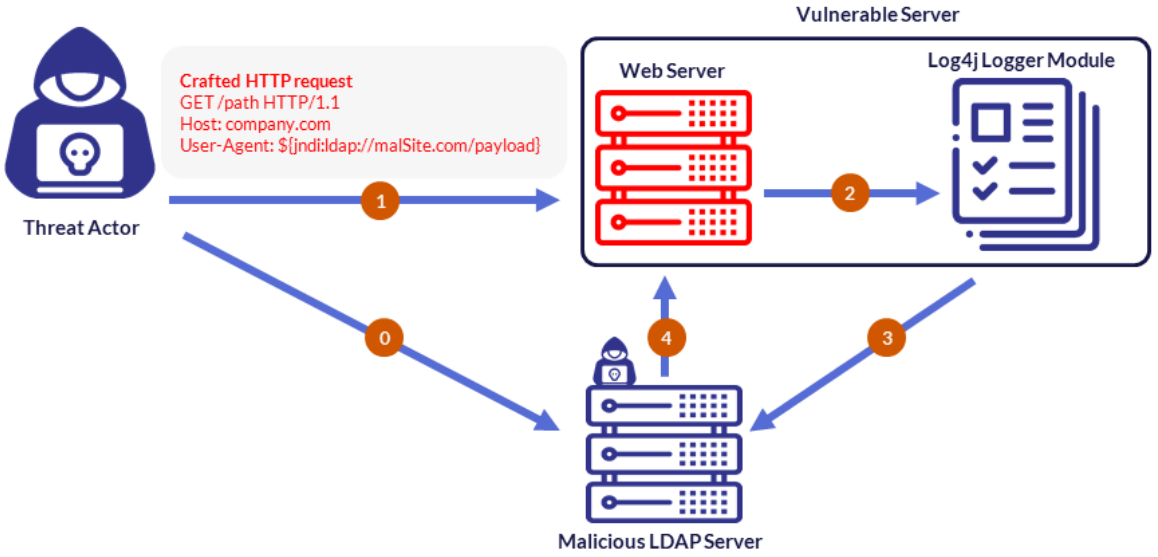
HITACHI
Inspire the Next



1984	Compilateur compromis (démo)
2010	NSA Cisco, Siemens/Stuxnet
2015	Heartbleed/SSL, Apple Xcode
2017	NotPetya, Struts (Equifax), CCleaner (Asus, Google, Microsoft, Akamai, Samsung, Sony, Vmware, HTC, Linksys, Dlink, Cisco, NetSarang, Zepetto, Electronics Extreme)
2018	SuperMicro
2019	Visual Studio (Microsoft)
2020	Solar Winds, NTT BHE, Atlassian (démo)
2021	Kaseya, Xcode (encore), Codecov, Github (démo), Mimecast/Office 365, Azure, Visual Studio (encore/démo), Compilateur compromis (démo)

Log4j

HITACHI
Inspire the Next



0. Threat actor setting up his malicious LDAP server with malicious Java class
1. Threat actor sends malicious payload that is likely to be logged by the application
2. Payload passed to Log4j for logging
3. Log4j parse the payload and make a query to the malicious LDAP server
4. The LDAP server responds with content that holds the malicious java class

NHTSA - « Pratiques exemplaires de cybersécurité pour la sécurité des véhicules modernes » (en anglais)

HITACHI
Inspire the Next

Cybersecurity Best Practices for the Safety of Modern Vehicles

Draft 2020 Update

U.S. Department of Transportation
National Highway Traffic Safety Administration

4.2.5 Protections

[G.8] For remaining functionality and underlying risks, layers of protection[17] that are appropriate for the assessed risks should be designed and implemented.

[G.9] Clear cybersecurity standards should be specified and communicated to the suppliers that support the intended protections.[18]

4.2.6 Inventory and Management of Software Assets on Vehicles

[G.10] Manufacturers should maintain a database of operational software components[19,20] used in each automotive ECU, each assembled vehicle, and a history log of version updates applied over the vehicle's lifetime.

[G.11] Manufacturers should track sufficient details related to software components,[21] such that when a newly identified vulnerability is identified related to an open source or off-the-shelf software,[22] manufacturers can quickly identify what ECUs and specific vehicles would be affected by it.

4.2.7 Penetration Testing and Documentation

[G.12] Manufacturers should evaluate all commercial off-the-shelf and open-source software components used in vehicle ECUs against known vulnerabilities.[23,24]

[G.13] Manufacturers should also pursue product cybersecurity testing, including using

that support the intended protections.[18]

4.2.6 Inventory and Management of Software Assets on Vehicles

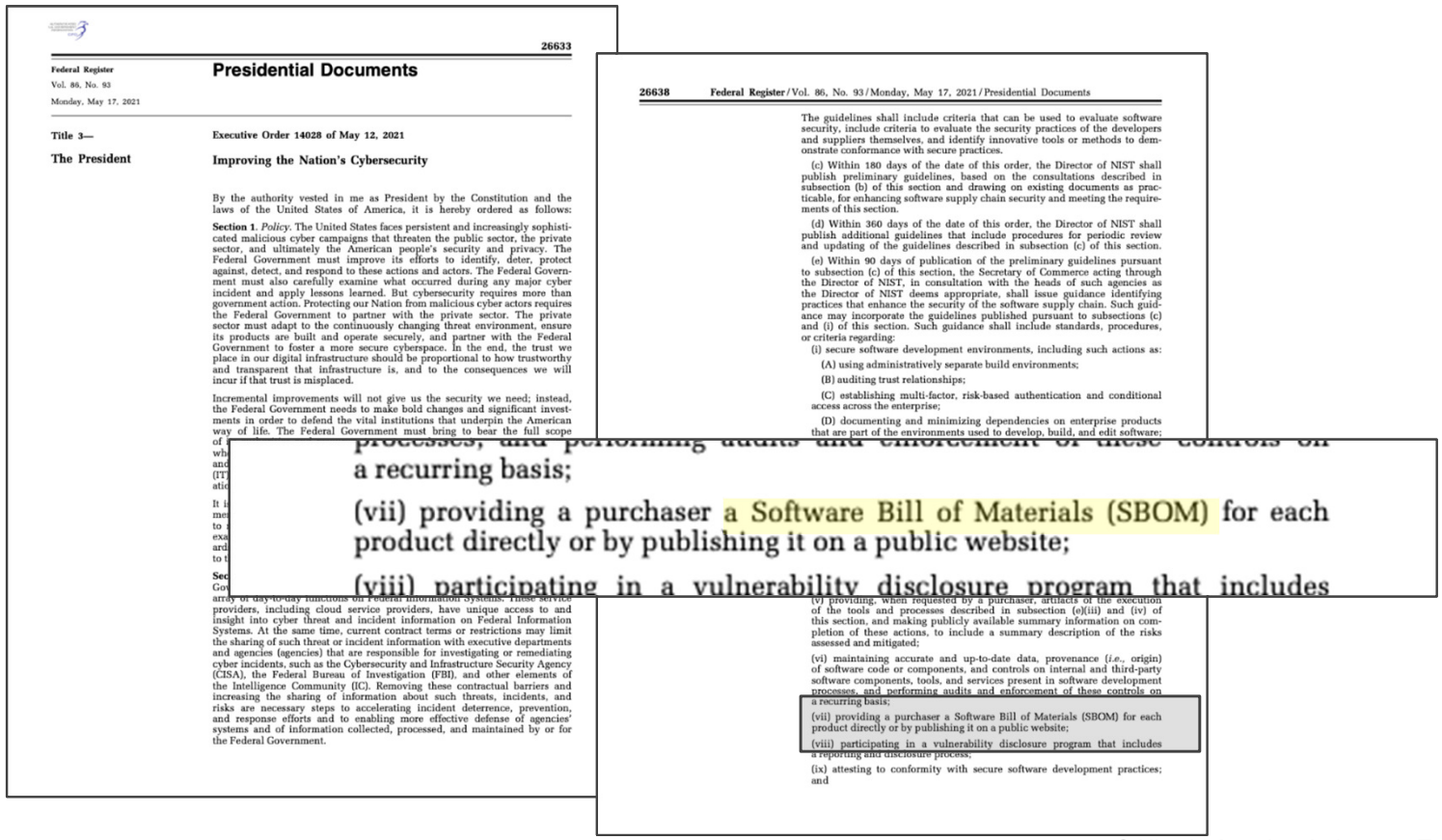
[G.10] Manufacturers should maintain a database of operational software components[19,20] used in each automotive ECU, each assembled vehicle, and a history log of version updates applied over the vehicle's lifetime.

[G.11] Manufacturers should track sufficient details related to software components,[21] such that when a newly identified vulnerability is identified related to an open source or off-the-shelf software,[22] manufacturers can quickly identify what ECUs and specific vehicles would be affected by it.

4.2.7 Penetration Testing and Documentation

Mai 2021 - Décret exécutif 14028 - « Améliorer la cybersécurité de la nation »

HITACHI
Inspire the Next



26633

Federal Register
Vol. 86, No. 93
Monday, May 17, 2021

Presidential Documents

Title 3—
The President

Executive Order 14028 of May 12, 2021

Improving the Nation's Cybersecurity

By the authority vested in me as President by the Constitution and the laws of the United States of America, it is hereby ordered as follows:

Section 1. *Policy*. The United States faces persistent and increasingly sophisticated malicious cyber campaigns that threaten the public sector, the private sector, and ultimately the American people's security and privacy. The Federal Government must improve its efforts to identify, deter, protect against, detect, and respond to these actions and actors. The Federal Government must also carefully examine what occurred during any major cyber incident and apply lessons learned. But cybersecurity requires more than government action. Protecting our Nation from malicious cyber actors requires the Federal Government to partner with the private sector. The private sector must adapt to the continuously changing threat environment, ensure its products are built and operate securely, and partner with the Federal Government to foster a more secure cyberspace. In the end, the trust we place in our digital infrastructure should be proportional to how trustworthy and transparent that infrastructure is, and to the consequences we will incur if that trust is misplaced.

Incremental improvements will not give us the security we need; instead, the Federal Government needs to make bold changes and significant investments in order to defend the vital institutions that underpin the American way of life. The Federal Government must bring to bear the full scope of

providers, including cloud service providers, have unique access to and insight into cyber threat and incident information on Federal Information Systems. At the same time, current contract terms or restrictions may limit the sharing of such threat or incident information with executive departments and agencies (agencies) that are responsible for investigating or remediating cyber incidents, such as the Cybersecurity and Infrastructure Security Agency (CISA), the Federal Bureau of Investigation (FBI), and other elements of the Intelligence Community (IC). Removing these contractual barriers and increasing the sharing of information about such threats, incidents, and risks are necessary steps to accelerating incident deterrence, prevention, and response efforts and to enabling more effective defense of agencies' systems and of information collected, processed, and maintained by or for the Federal Government.

26638 Federal Register / Vol. 86, No. 93 / Monday, May 17, 2021 / Presidential Documents

The guidelines shall include criteria that can be used to evaluate software security, include criteria to evaluate the security practices of the developers and suppliers themselves, and identify innovative tools or methods to demonstrate conformance with secure practices.

(c) Within 180 days of the date of this order, the Director of NIST shall publish preliminary guidelines, based on the consultations described in subsection (b) of this section and drawing on existing documents as practicable, for enhancing software supply chain security and meeting the requirements of this section.

(d) Within 360 days of the date of this order, the Director of NIST shall publish additional guidelines that include procedures for periodic review and updating of the guidelines described in subsection (c) of this section.

(e) Within 90 days of publication of the preliminary guidelines pursuant to subsection (c) of this section, the Secretary of Commerce acting through the Director of NIST, in consultation with the heads of such agencies as the Director of NIST deems appropriate, shall issue guidance identifying practices that enhance the security of the software supply chain. Such guidance may incorporate the guidelines published pursuant to subsections (c) and (i) of this section. Such guidance shall include standards, procedures, or criteria regarding:

(i) secure software development environments, including such actions as:

(A) using administratively separate build environments;

(B) auditing trust relationships;

(C) establishing multi-factor, risk-based authentication and conditional access across the enterprise;

(D) documenting and minimizing dependencies on enterprise products that are part of the environments used to develop, build, and edit software;

a recurring basis;

(vii) providing a purchaser a Software Bill of Materials (SBOM) for each product directly or by publishing it on a public website;

(viii) participating in a vulnerability disclosure program that includes

(v) providing, when requested by a purchaser, artifacts of the execution of the tools and processes described in subsection (e)(iii) and (iv) of this section, and making publicly available summary information on completion of these actions, to include a summary description of the risks assessed and mitigated;

(vi) maintaining accurate and up-to-date data, provenance (*i.e.*, origin) of software code or components, and controls on internal and third-party software components, tools, and services present in software development processes, and performing audits and enforcement of these controls on a recurring basis;

(vii) providing a purchaser a Software Bill of Materials (SBOM) for each product directly or by publishing it on a public website;

(viii) participating in a vulnerability disclosure program that includes a reporting and disclosure process;

(ix) attesting to conformity with secure software development practices; and

Principaux règlements et orientations

HITACHI
Inspire the Next

- **Il n'y a pas de réglementation SBOM actuelle dans l'industrie automobile.**
- Mais il y a un intérêt croissant (par exemple, la « pratique exemplaire » de la NHTSA)
- Remarque : Le décret exécutif ne s'applique qu'aux achats et opérations du gouvernement américain - il ne constitue pas une force de loi

Orientations des gouvernements

- Les **États-Unis** sont le principal moteur mondial, influençant les alliés et les fournisseurs commerciaux américains
  - DoC - **Programme multipartite public/privé de la NTIA**, orientation du NIST pour le gouvernement américain et l'industrie privée
  - DHS - CISA - Prochaine phase d'orientation et de réglementation du SBOM
  - DoE - Validation de principe SBOM démarrant sous la supervision de l'INL et du PNNL
  - DoD - Longtemps requis pour les documents classifiés, récemment étendu pour les documents non classifiés, étendu davantage par le décret exécutif 14028
  - FDA - Publication d'un projet d'orientation de précommercialisation pour les dispositifs médicaux
  - DoT - NHTSA - Pratiques exemplaires en matière de cybersécurité (qui devraient passer de facultatives à obligatoires). Le Département des Transports envisage de l'exiger pour tous les achats de véhicules fédéraux
  - EOP - NSC, OMB, d'autres qui dirigent la mise en conformité des agences selon les décrets et autres directives
- Le Ministère de l'Économie, du Commerce et de l'Industrie (METI) **du Japon**, l'ENISA **de l'UE** et d'autres organismes envisagent des orientations - probablement similaires à celles des États-Unis

Orientations des organismes de normalisation

- **ISO** - Pas encore d'exigences, mais nécessite une analyse de risque du code dans la norme 21434
- **UNECE WP.29 -** Pas encore d'exigences, mais la R155 exige la démonstration des risques liés aux fournisseurs

HITACHI
Inspire the Next

SBOM et Automotive ISAC

Contexte - ISAC (centres d'analyse et de partage de l'information)

HITACHI
Inspire the Next

- Préoccupations de l'après-11 septembre concernant le risque systémique dans l'industrie américaine
- La directive 21 de la politique présidentielle a demandé au DHS d'encourager la coopération et la coordination entre le secteur public et le secteur privé et a énuméré les premiers secteurs d'infrastructures essentielles
- Le Département américain de la sécurité intérieure a ensuite désigné 16 secteurs d'infrastructures essentielles américains en particulier
- L'industrie automobile et les industries connexes sont désignées comme faisant partie du secteur de la production essentielle (sans être spécifiquement désignées comme un secteur unique)
- L'avantage juridique des ISAC est la sphère de sécurité antitrust. Le plus grand avantage est la communauté d'industriels et de spécialistes de la cybersécurité.

Important : « 16 » secteurs d'infrastructures essentielles

HITACHI
Inspire the Next

« Il existe 16 secteurs d'infrastructures essentielles dont les actifs, les systèmes et les réseaux, qu'ils soient physiques ou virtuels, sont considérés comme si vitaux pour les États-Unis que leur incapacité ou leur destruction aurait un effet débilitant sur la sécurité, la sécurité économique nationale, la santé ou la sécurité publique nationale, ou toute combinaison de ces éléments. »

https://www.cisa.gov/critical-infrastructure-sectors

- Produits chimiques
- Communications
- Barrages
- Services d'urgence
- Services financiers
- Installations gouvernementales
- Technologies de l'information
- Systèmes de transport
- Installations commerciales
- Production essentielle
- Base industrielle de la défense
- Énergie
- Alimentation et agriculture
- Installations gouvernementales
- Soins de santé et santé publique
- Réacteurs, matériaux et déchets nucléaires
- Systèmes d'eau et d'eaux usées

Groupe de travail Auto-ISAC SBOM - Historique

HITACHI
Inspire the Next

Phase 1 - mars-juillet 2019

Promoteur : Analyste du groupe de travail

Objectif : Veiller à ce que le NTIA SBOM tienne compte des questions et des opinions de l'industrie automobile

Équipe : 10 membres (dont 3 équipementiers)

Objectif : Publier les préoccupations à la NTIA et défendre l'industrie automobile

Phase 2 - nov 2020 à aujourd'hui

Promoteur : Groupe d'affinité des fournisseurs

Objectif : Se mettre d'accord sur les pratiques exemplaires parmi les fournisseurs et proposer des solutions aux équipementiers

Équipe : 17 membres (1 équipementier)

Objectifs :

- Une voix unifiée des fournisseurs sur l'adoption du SBOM auprès des équipementiers
- S'aligner sur la NTIA
- Approche pratique avec la contribution des équipementiers
- Pratiques exemplaires publiées en 2021

Auto-ISAC AWG SBOM SIG (Phase 1) - 2019
Objectif : Les problèmes des membres abordés avec la NTIA

HITACHI
Inspire the Next

1. Quelles sont les **informations nécessaires** sur un SBOM pour fournir une analyse, des conseils de partage et la sécurité?
2. Quelles **informations sont partagées** avec les consommateurs du composant?
3. Comment les **composants** sont-ils **classés** dans un SBOM?
4. Comment les **composants** sont-ils **identifiés**, par exemple la version, la branche, le fragment, le fournisseur/auteur?
5. Quel est l'équilibre entre **transparence et responsabilité?**
6. Comment **protéger la propriété intellectuelle** dans une nomenclature transparente?
7. Une nomenclature doit-elle **énumérer toutes les variantes**?
8. **Qui obtient le SBOM** et par quels moyens?
9. Comment **distinguer** les **sous-composantes des** grandes bibliothèques **de l'utilisation générale de** la bibliothèque?
10. Comment **Auto-ISAC interagira-t-il avec les** autres **projets du SBOM** et les influencera-t-il?
11. Comment les composants seront-ils **identifiés, suivis et audités par le consommateur** du composant?
12. Comment les **équipes d'ingénierie logicielle et d'assurance qualité fourniront-elles les SBOM?**
13. Comment les **agents d'achat** vont-ils **appliquer les pratiques exemplaires du SBOM** et bloquer les composants à accès restreint?

Aperçu : Proposition de guide des pratiques exemplaires

HITACHI
Inspire the Next

COMPRENDRA

- Distribution TLP:AMBRE (pour l'instant)
- Chevauchement substantiel avec les orientations de la NTIA
- Personnalisations pour l'automobile
- Mise en correspondance avec le cycle de vie des produits automobiles
- Format et recommandations opérationnelles
- Partage de la discussion
- Liste d'outils neutres pour les fournisseurs
- Bibliographie, formation et documents de référence

NE COMPRENDRA PAS

- Règles obligatoires - tous les points seront des recommandations
- Usurpation des contrats ou des exigences des fournisseurs
- Orientation statique - révisions prévues au cours de la phase 3 et en cours

Les arguments contre le SBOM - Les grandes objections

HITACHI
Inspire the Next

1. **Problèmes relatifs à la propriété intellectuelle**
   - Délivrance de permis et de licences
   - Informations anticoncurrentielles
   - Violation d'autres clauses du contrat
   - Avantage commercial ou négociation déloyale pour le consommateur
2. **Problèmes juridiques, de responsabilité et de réglementation**
3. **Faciliter le piratage**

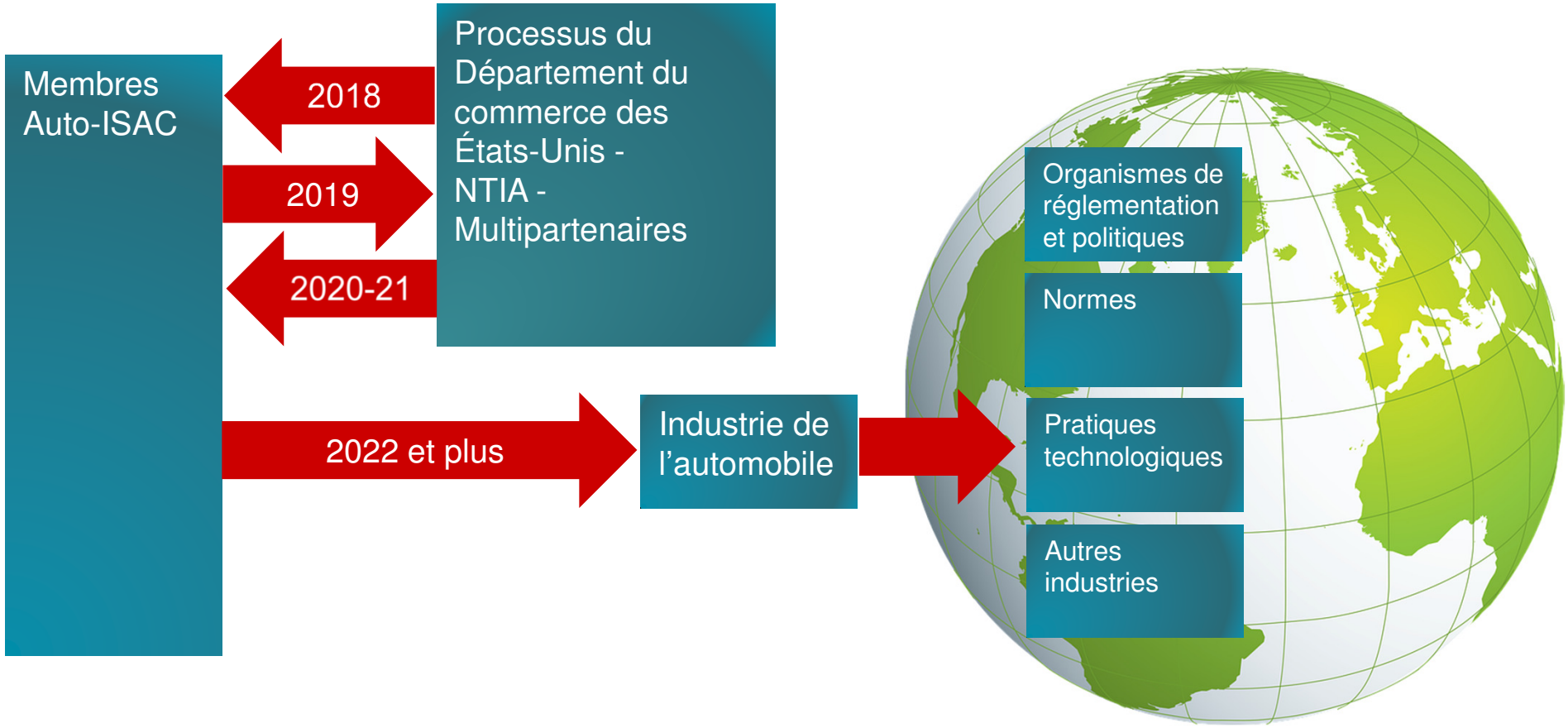
Toutes ont été conciliées (ou presque) avec les préoccupations des membres dans le projet de guide des pratiques exemplaires

Prochaines étapes

HITACHI
Inspire the Next

1. **Finaliser le projet de proposition de pratiques exemplaires (fait)**
2. **Approbation du conseil d'administration**
3. **Phase 3 (probable) - exercice actif - détails en cours de discussion**
4. **Possibilités futures (non décidées)**
   - Exercice pilote de production limitée
   - Programme de formation
   - Automatisation et essais d'outils
   - Programme DHS/CISA (successeur de la NTIA)
   - Exercice d'intégrité de la chaîne d'approvisionnement
   - Cas d'utilisation et exercice de gestion des vulnérabilités
   - Ajout de l'automatisation de Vulnerability/Exploitability eXchange (VEX)

Coopération, éducation et orientation




HITACHI
Inspire the Next

HITACHI
Inspire the Next

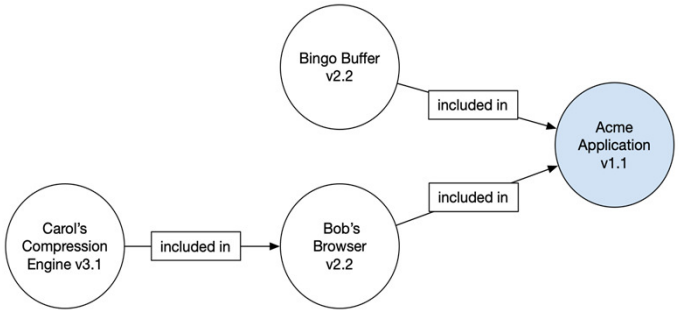
Introduction - nomenclature logicielle

Nomenclature logicielle (SBOM)

HITACHI
Inspire the Next

SBOM : Un inventaire formel, lisible par machine, des composants logiciels et de leurs dépendances, des informations sur ces composants et leurs relations hiérarchiques.

- Inventaire exhaustif (ou indiquer explicitement où il ne l'est pas)
- Peut inclure des logiciels libres ou des logiciels propriétaires
- Peut être largement ou publiquement disponible, ou à accès restreint



Nom du composant	Nom du fournisseur	Chaîne de version	Auteur	Condensé numérique	UID	Relation
Application	Acme	1,1	Acme	0x123	234	Lui-même
|--- Navigateur	Bob	2.1	Bob	0x223	334	Inclus dans
|--- Moteur de compression	Carol	3.1	Acme	0x323	434	Inclus dans
|--- Tampon	Bingo	2.2	Acme	0x423	534	Inclus dans

Historique :
2018 : Améliorations de la sécurité exigées par la FDA.
2019 à 2021 : Orientation du DoC NTIA
2021 : Exigé par le gouvernement américain et d'autres
2022 : Guide des pratiques exemplaires d'Auto-ISAC

Points clés pour l'industrie automobile

1. **S'applique aux logiciels embarqués, aux micrologiciels et aux microcodes**
2. **Aspect important de la sécurité pour la chaîne d'approvisionnement technologique**

Données de base du SBOM - « Minimum Viable Product » (produit minimum viable)

HITACHI
Inspire the Next

Nom de l'auteur	Auteur du SBOM
Nom du fournisseur	L'entité qui est responsable du soutien de l'objet du SBOM. Vendeur, fabricant, développeur, responsable de la maintenance, distributeur, etc.
Nom du composant	Le fournisseur ou l'auteur décide
Chaîne de version	Le fournisseur décide
Condensé numérique du composant	Vérification du code cryptographique pour s'assurer que le composant correspond aux références du SBOM
Identifiant unique	CPE, purl, UUID, GUID, etc
Relation	« Soi-même » est le composant qui fait l'objet du SBOM. « Inclus dans » fait référence à un autre composant du SBOM.

Quels sont les formats utilisés pour spécifier les SBOM?

HITACHI
Inspire the Next

- **SPDX - Échange de données sur les progiciels https://spdx.dev**
  - Parrainé par la Fondation Linux
  - Destiné à l'origine au catalogue de licences à code source ouvert
  - Soutien robuste
  - Adaptation spécialement conçue pour le SBOM par la Fondation Linux
- **SWID - Software Identification (balise) https://csrc.nist.gov/projects/Software-Identification-SWID**
  - ISO/CEI 19770-2
  - Destiné au suivi des stocks, il fonctionne également pour le SBOM
  - Soutien du NIST, l'information complète nécessite un abonnement à l'ISO ou à la CEI
  - Balisage des attributs logiciels
- **CycloneDX - https://cyclonedx.org**
  - Groupe de travail principal de l'OWASP CycloneDX
  - Extensions disponibles pour les environnements de programmation
  - Support SBOM natif étendu (c.-à-d. superposé aux directives de la NTIA)
  - Bonne assistance, programme récent, mais très développé